CONSTRAINTS ON HYPOTHETICAL COUNTEREXAMPLES TO THE CASAS-ALVERO CONJECTURE

R. LATERVEER & M. OUNAIES

In [1], Casas-Alvero formulated the following :

Conjecture. *Let $f \in \mathbb{C}[X]$ be a polynomial of degree $N \geq 1$. Assume that f has a common root with each of its derivatives $f^{(1)}, \cdots, f^{(N-1)}$ (we will say that f is CA). Then f is of the form $f(z) = a(z - b)^N$, $a, b \in \mathbb{C}$.*

The conjecture is known to be true in low degrees [3]. The first major break-through in the subject was [5], where the conjecture is proven for all N that are powers of a prime number. A very nice overview of all that is currently known concerning this conjecture, as well as an alternative proof of the result of [5], can be found in [4].

This note is the fruit of a failed attempt to prove the conjecture for $N = 12$ (this is the lowest degree for which the conjecture has not been settled as yet).

What follows is a short description of the contents of this note.

In the first section, which is largely expository, techniques are elementary. The degree N is arbitrary, and we ask ourselves under what extra conditions on the number of roots the conjecture can be proven: The main new result in this first section is proposition 5: the conjecture is true if f has at most 4 distinct roots.

In the second section we restrict attention to the case $N = p^r + 1$ (where p is a prime), and then further specialize to the case $N = p + 1$. We use the p-adic valuation, inspired by Draisma and de Jong's take ([4], [6]) on the result of Graf von Bothmer et alii [5]. The main results of the second section are: If f is a CA-polynomial of degree $N = p + 1$, and c is the root of $f^{(N-1)}$, then there are at least 2 other indices $2 \leq l_1 < l_2 < N - 1$ such that $f^{(l_1)}(c) = f^{(l_2)}(c) = 0$ (this is Proposition 7). Also, we are able to prove the conjecture for degree $p + 1$ polynomials all of whose roots are rational (Proposition 8).

In the third and last section, we present a short remark that gives some additional constraints on hypothetical counterexamples to the conjecture in degree 12.

We hope this note may raise interest in the subject, and perhaps spark further progress towards proving the conjecture...

Convention. *In what follows, we will call a polynomial non-trivial if it has at least two distinct roots. The conjecture says that there exists no non-trivial CA-polynomial.*

From the definition of a CA-polynomial, it is easily seen that:

Lemma 1. *Let f be a monic CA-polynomial of degree $N \geq 1$ and $\alpha \in \mathbb{C}^*$ and $\beta \in \mathbb{C}$. The polynomial $g(z) = \alpha^{-N} f(\alpha z + \beta)$ is also a monic CA-polynomial of degree N.*

In consequence, whenever convenient, we may choose any root of f and assume it to be equal to 0. When we have two distinct roots of f, we may assume the first to be equal to 0 and the second to be equal to 1.

1. CONSTRAINTS ON THE NUMBER OF DISTINCT ROOTS

The following result, proven by Draisma and de Jong, conveniently subsumes many "easy" cases where the conjecture can be proven:

Proposition 1. [4, Proposition 6] *Let f be a CA-polynomial of degree $N \geq 1$. Let α_i, $i = 1, \cdots, N-1$ be a common root of f and $f^{(i)}$. Then the cardinality of $\{\alpha_1, \cdots, \alpha_{N-1}\}$ cannot be two.*

Remark 1. *As immediate corollaries of Proposition 1, we get the following three special cases:*
1. *If f is CA and $f''(z) = N(N-1)(z-a)^{N-2}$, then $f(z) = (z-a)^N$.*
2. *Let f be a monic CA-polynomial of degree N, and suppose that f has a root a of multiplicity at least $N-1$. Then $f(z) = (z-a)^N$.*
3. *Let f be a non-trivial CA-polynomial, then f has at least three distinct roots.*
   We note that case 1 was also dealt with in [11, Proposition 2.2].

In the next two propositions, we will go a step further in directions 1 and 2. Later on (Propositions 4 and 5), we will go two steps further in direction 3.

Proposition 2. *Let f be a CA-polynomial of degree $N \geq 4$. Assume that for some $a \in \mathbb{C}$, $f^{(3)}(z) = \frac{N!}{(N-3)!}(z-a)^{N-3}$. Then $f(z) = (z-a)^N$.*

Proof. Thanks to Lemma 1, we may choose $a = 0$.

Assume that $f'(0) \neq 0$, then f has a root of multiplicity at least 2 which is different from 0 and again by Lemma1, we may assume $f(1) = f'(1) = 0$. Thus

$$f(z) = z^N - (N-1)z^2 + (N-2)z; \quad f''(z) = (N-1)\left(Nz^{N-2} - 2\right).$$

Solving $f(z) = f''(z) = 0$, we get $z = \frac{N}{N+1}$ and $\left(\frac{N+1}{N}\right)^{N-2} = \frac{N}{2}$. We easily see that the function $\phi(t) = (t-2)\ln\frac{t+1}{t} - \ln\frac{t}{2}$ is strictly decreasing for $t \geq 4$ and that $\phi(4) < 0$. Thus the equality $\phi(N) = 0$ is never reached for $N \geq 4$.

We conclude that we necessarily have $f'(0) = 0$. Then, for some constant c, $f''(z) = N(N-1)z^{N-2} + 2c$ and $f(z) = z^N + cz^2$. Solving $f(z) = f''(z) = 0$, we get that $c = 0$. $\qquad\square$

Proposition 3. *Let f be a monic CA-polynomial of degree $N \geq 3$, and suppose f has a root a of multiplicity at least $N-2$. Then $f(z) = (z-a)^N$.*

Proof. Let $a = 0$. If $f^{(N-1)}(0) \neq 0$, then we may assume that $f(1) = f^{(N-1)}(1) = 0$. Hence

$$f(z) = z^{N-2}(z^2 - Nz + N - 1), \quad f^{(N-2)}(z) = \frac{(N-1)!}{2}(Nz^2 - 2Nz + 2).$$

Solving $f(z) = f^{(N-2)}(z) = 0$, we get $z^2 = 2$ and $z = \frac{N+1}{N}$. Thus $(N+1)^2 = 2N^2$ which is impossible.

We conclude that we necessarily have $f^{(N-1)}(0) = 0$. Then, for some constant c, $f(z) = z^N + cz^{N-2}$ and $f^{(N-2)}(z) = \frac{N!}{2}z^2 + c$. Solving $f(z) = f^{(N-2)}(z) = 0$, we get $c = 0$. $\qquad\square$

Remark 2. *We have chosen to present an elementary proof of Proposition 3, though we also can see it as direct consequence of the forthcoming Proposition 4.*

Now, before going further, let us recall some basic properties of the elementary symmetric polynomials. Let a polynomial f and its derivatives be of the form

$$f^{(l)}(z) = \frac{N!}{N-l!}\left(a_0 z^{N-l} + \binom{N-l}{1}a_1 z^{N-l-1} + \binom{N-l}{2}a_2 z^{N-l-2} + \cdots + a_{N-l}\right).$$

(Here by convention $f = f^{(0)}$). Let $\sigma_m(l)$ be the sum of the mth powers of the roots of $f^{(l)}$, for $l = 0, \cdots, N-1$. Then Newton formulas applied to each $f^{(l)}$ give the following relations (See for example [7] for more details on Newton formulas):

Lemma 2.

$$\sum_{k=1}^{j} \sigma_k(l)\binom{N-l}{j-k}a_{j-k} = -j\binom{N-l}{j}a_j$$

for $0 \le l \le N-1$, $1 \le j \le N-l$.

Remark 3. *In particular, for $j = 1$, we have that*

$$\frac{\sigma_1(l)}{N-l} = \frac{\sigma_1(0)}{N}$$

for $l = 0, \cdots, N-1$, which means that the center of mass of the roots of the derivatives is fixed. As obviously

$$\sigma_1(N-1) = \frac{\sigma_1(0)}{N} = a_1$$

is the only root of $f^{(N-1)}$, we see that whenever f is a Casas-Alvero polynomial, the center of mass of its roots $\dfrac{\sigma_1(0)}{N}$ is itself a root of f. As a direct consequence, the number of distinct roots of a Casas-Alvero polynomial cannot be two. Actually, we can say more: if f has more than two distinct roots, then at least one of them (the center of mass) has to be in the interior of the convex hull of the roots.

In order to go further in the study of this convex hull, let us first recall the well-known Gauss-Lucas theorem:

Theorem 1 (Gauss-Lucas). *Let $f \in \mathbb{C}[X]$. Let f be a complex polynomial, f' be its derivative and Γ be the convex hull of the roots of f. Then each root of f' is either a multiple root of f, or belongs to the interior of Γ.*

We will call the convex hull Γ of the roots of f the *Gaus-Lucas hull* of f, the interior of Γ the *open Gauss-Lucas hull* and the boundary of Γ the *Gauss-Lucas polygon*.

Corollary 1. [8] *Let f be a polynomial of degree N. Let ζ be a root of f located on its Gauss-Lucas polygon, with multiplicity $m \leq N - 1$. Then, for all $m \leq k \leq N - 1$, $f^{(k)}(\zeta) \neq 0$.*

This corollary yields another way of seeing that a non-trivial CA-polynomial f must have at least one of its roots in its open Gauss-Lucas hull, and in particular that the number of distinct roots cannot be two. Actually, we can also use Gauss-Lucas theorem to show that this number cannot be three either and more generally that a non-trivial CA-polynomial must have at least two distinct roots in its open Gauss-Lucas hull.

Proposition 4. *Let f be a non-trivial Casas-Alvero polynomial of degree $N \geq 3$. Then f has at least two distinct roots in its open Gauss-Lucas hull. In particular, $N \geq 5$ and f has at least 4 distinct roots.*

Proof. Assume that f has exactly one root, say 0, in its open Gauss-Lucas hull and let ζ be the one among the roots of f located on the Gauss-Lucas polygon with maximal multiplicity m. Then by Corollary 1, $f^{(m)}(0) = f^{(m+1)}(0) = \cdots = f^{(N-1)}(0) = 0$ which means that for $j = m, \ldots, N - 1$:

$$f^{(j)}(z) = \frac{N!}{(N-j)!} z^{N-j}.$$

Taylor expansion gives

$$f(0) = \sum_{j=m}^{N} \frac{f^{(j)}(\zeta)}{j!} (-\zeta)^j = \zeta^N \sum_{j=m}^{N} (-1)^j \binom{N}{j} = \zeta^N (-1)^m \binom{N-1}{m}.$$

As $f(0) = 0$, we get $\zeta = 0$, which is a contradiction. $\qquad\square$

Remark 4. *Proposition 4 can also be deduced from Draisma and de Jong's result Proposition 1.*

As pointed out in [4], arguments based only on Gauss-Lucas theorem are not sufficient to deal with polynomials of degree greater than 5. In the next proposition, we will use Rolle's theorem and relations 2 to go further :

Proposition 5. *Let f be a non-trivial Casas-Alvero polynomial of degree $N \geq 5$. Then f has at least five distinct roots. In particular, $N \geq 6$.*

Proof. Assume that f has four distinct roots. Then by the previous proposition, it has at least two distinct roots in its open Gauss-Lucas hull. This implies that the four roots are on a line. By Lemma 1, we may assume that it is the real line. Then by Gauss-Lucas theorem, all its derivatives also have only real roots. We will use the following lemma based on Rolle's theorem :

Lemma 3. [9, Lemma 4.2] *A root of multiplicity m of f, $0 \leq m \leq i$ can be at most a simple root of $f^{(i)}$.*

We denote by M the maximal multiplicity of the roots of f. By Proposition 3, we know that $2 \leq M \leq N - 3$.

- First case : $M \leq N-5$. Again using Lemma 1, we may assume without loss of generality that the roots of f are as follows : $a < 0 < 1 < b$ and $f^{(N-1)}(0) = 0$. By Corollary 1, a and b cannot be zeros of $f^{(k)}$ for $N - 5 \leq k \leq N - 1$. Besides, by Lemma 3, each zero of $f^{(k)}$ is simple. Then we necessarily have $f^{(N-2)}(1) = 0$, $f^{(N-3)}(0) = 0$, $f^{(N-4)}(1) = 0$, $f^{(N-5)}(0) = 0$. Integrating five times the expression $f^{(N-1)}(z) = N!z$ and taking into account these constraints, we get $f^{(N-5)}(z) = \dfrac{N!}{5!}z(z^2 - 5)^2$. But this contradicts Lemma 3.

- Second case : $M = N - 4$ (which implies that $N \geq 6$). By Lemma 1, we arrange the roots as follows : $a < 0 < b < 1$ and we assume that $f^{(N-1)}(0) = 0$. Denote by m_a, m_0, m_b, m_1 their respective multiplicities. Then again by Lemma 3, we must have $f^{(N-2)}(b) = 0$, $f^{(N-3)}(0) = 0$, $f^{(N-4)}(b) = 0$. Like in the first case, computing the last derivatives, we get

$$f^{(N-1)}(z) = N!z, \quad 2!f^{(N-2)}(z) = N!(z^2 - b^2),$$
$$3!f^{(N-3)}(z) = N!z(z^2 - 3b^2), \quad 4!f^{(N-4)}(z) = N!z(z^2 - 5b^2)(z^2 - b^2).$$

Obviously, as $f^{(N-4)}(b) = 0$, we have $m_b \leq N - 5$. From Gauss-Lucas theorem, we deduce that $a < -\sqrt{5}b$. Now we apply Lemma 2 with $l = 0$, $j = 1$ and with $l = 0$, $j = 3$ to obtain

$$(1) \qquad m_a a + m_b b + m_1 = m_a a^3 + m_b b^3 + m_1 = 0.$$

We deduce that $m_a a(a^2 - 1) = -m_b b(b^2 - 1)$ and looking at the sign, we see that $-a < 1$. Then $m_a > -am_a = m_b b + m_1 > m_1$ which implies that $m_a \geq 2$ and $m_1 \leq N - 5$.

Let us note that in the case where $m_a = 2, m_1 = m_b = 1$, equations 1 give : $a(a+1)^2 = 0$.

Thus, this case cannot occur. We can readily deduce that $m_0 \leq N - 5$. The only possibility left is $m_a = M = N - 4$.

From the relation $-(N - 4)a(1 - a^2) = m_b b(1 - b^2)$, we deduce that $\phi(-a) \leq \phi(b)$ where we put $\phi(t) = t(1 - t^2)$. But ϕ is increasing on $[0, 1/\sqrt{3}]$ and we know that $-a > b > 0$. Thus we have $-a > 1/\sqrt{3}$. Now we get back to the linear equation in 1 :

$$N - 4 = m_b \frac{b}{-a} + m_1 \frac{1}{-a} < \frac{m_b}{\sqrt{5}} + m_1\sqrt{3}.$$

If $m_1 = m_b = 1$, this leads to $N = 6$ and $m_a = 2$. But we have already shown above that this case can't occur.

If $m_1 = 1$, $m_b = 2$, we also obtain $N = 6$ and $m_a = 2$.

Equations 1 now imply that $4a^2 + 2a - 1 = 0$. But this equation has no real solution.

If $m_1 = 2$, $m_b = 1$, we obtain $N \leq 7$. On the other hand, we know that $m_1 \leq N - 5$. Thus $N = 7$ and $m_a = 3$.

Equations 1 imply $(a+1)^2(4a+1) = 0$. Thus we must have $a = -1/4$ and $b = -5/4$. But this contradicts the fact that $b > 0$.

Finally, the second case leads to a contradiction.

- Third case : $M = N - 3$. We proceed similarly to the previous case. Again, we obtain that $m_a \geq 2$. Thus we necessarily have : $m_a = M$, $m_0 = m_1 = m_b = 1$. The linear equation in 1 gives :

$$N - 3 = \frac{b}{-a} + \frac{1}{-a} < \frac{1}{\sqrt{5}} + \sqrt{3} < 3.$$

It follows that $N = 5$ and $m_a = 2$. But we have already shown that this is impossible.

$\square$

2. POLYNOMIALS OF DEGREE $p^r + 1$

We quickly recall the definition of the p-adic valuation (for more details, the reader is referred to [10])

Definition 1. *Let p be a prime number. For a positive integer $n \in \mathbb{N}^*$, the p-adic valuation $v_p(n)$ is defined to be the exponent of p in the prime decomposition of n: If $n = p^r \cdot n'$ with n' prime to p, then $v_p(n) = r$.*

The map $v_p \colon \mathbb{N}^* \to \mathbb{N}$ can be extended to a map $v_p \colon \mathbb{C} \to \mathbb{Q} \cup \{+\infty\}$ ([10, Chapter 4, Theorem 1]). This map satisfies the following properties:

- $v_p(c) = +\infty$ if and only if $c = 0$;
- $v_p(ab) = v_p(a) + v_p(b)$ for all a, b in $\mathbb{C}$;
- $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$ for all a, b in $\mathbb{C}$.

Remark 5. *It is important to note that the last property implies : $v_p(a + b) = \min\{v_p(a), v_p(b)\}$ if $v_p(a) \neq v_p(b)$.*

We will make a frequent use of this fact.

Lemma 4. [5, Lemma 2.4] *Let $r \geq 1$ be an integer and p be a prime number. Then $v_p(\binom{p^r}{j}) \geq 1$ for $1 \leq j \leq p^r - 1$.*

From the relation $v_p(\binom{p^r+1}{k}) = v_p(\binom{p^r}{k-1} + \binom{p^r}{k})$ we immediately deduce :

Lemma 5. *Let p be a prime, and suppose $N = p^r + 1$. Then*

$$v_p\left(\binom{N}{k}\right) \geq 1$$

for $2 \leq k \leq N - 2$.

Proposition 6. *Let p be a prime number and let f be a non-trivial polynomial of degree $N = p^r + 1$. Assume that f has a common root with $f^{(2)}, \cdots, f^{(N-1)}$. Let c be the center of mass of f. Then the following conditions are satisfied :*

- $f'(c) \neq 0$,
- *If $p \geq 3$, there is no $w \in \mathbb{C}^*$ such that $f(c - w) = f(c + w) = 0$,*
- *If $p \geq 3$, there is no $w \in \mathbb{C}^*$ such that $f'(c - w) = f'(c + w) = 0$.*

Proof. We may assume without loss of generality, using Lemma 1, that f is of the form

$$f(z) = z^N + \binom{N}{2} a_2 z^{N-2} + \cdots + \binom{N}{k} a_k z^{N-k} + \cdots + \binom{N}{2} a_{N-2} z^2 + a_{N-1} z$$

and that $\min\{v_p(z_j),\ j = 1, \cdots, N\} = 0$, where we have denoted by $z_1, z_2, \cdots, z_{N-1}, z_N = 0$ the zeros of f.

For $l = 1, \cdots, N-1$, we have:

(2) $$\frac{l!}{N!} f^{(N-l)}(z) = z^l + \binom{l}{2} a_2 z^{l-2} + \cdots + \binom{l}{k} a_k z^{l-k} + \cdots + \binom{l}{1} a_{l-1} z + a_l.$$

Following the proof of [4, Proposition 9], using equality (2) with $l = 2, \cdots, N-2$ and z the common root of $f^{(N-l)}$ and f, we prove by induction on l that

(3) $$v_p(a_l) \geq 0 \quad \text{for all } l = 2, \cdots, N-2.$$

Let z_j be such that $v_p(z_j) = 0$. The equality

$$-a_{N-1} z_j = z_j^N + \binom{N}{2} a_2 z_j^{N-2} + \cdots + \binom{N}{k} a_k z_j^{N-k} + \cdots + \binom{N}{2} a_{N-2} z_j^2$$

shows that $v_p(a_{N-1}) = 0$. In particular, $f'(0) \neq 0$. Besides, as $a_{N-1} = \prod_{j=0}^{N-1} z_j$, we have $v_p(z_j) = 0$ for $j \in \{1, \cdots, N-1\}$.

If $p \geq 3$, we can also see that it is not possible to have a non-zero complex number w such that $f(w) = f(-w) = 0$. Indeed, otherwise, $0 = f(w) - f(-w)$ would give the identity :

$$-a_{N-1} w = \binom{N}{3} a_3 w^{N-3} + \binom{N}{5} a_5 w^{N-5} + \cdots + \binom{N}{3} a_{N-3} w^3$$

which contradicts (14).

We can use the same argument to show that there is no complex number w such that $f'(w) = f'(-w) = 0$. □

Remark 6. *For $N = p + 1$, it has been noted independently by Castryck that there is no non-trivial CA–polynomial of degree N whose center of mass coincides with its double root [2, Lemma 9].*

From now on, we will assume that f is a non-trivial CA-polynomial of degree $N = p + 1$ where $p \geq 3$ is a prime number.

Using once again Lemma 1, we may assume that

(4) $$\begin{cases} f(z) = z^N + N a_1 z^{N-1} + \binom{N}{2} a_2 z^{N-2} + \cdots + \binom{N}{k} a_k z^{N-k} + \cdots + \binom{N}{2} a_{N-2} z^2, \\ \\ N = p + 1,\ \min\{v_p(z_j),\ j = 1, \cdots, N\} = 0, \end{cases}$$

where we have denoted by $z_1, \cdots, z_{N-3}, z_{N-2} = z_{N-1} = 0, z_N = -a_1$ the roots of f.

For $l = 1, \cdots, N-1$, we have:

(5) $\dfrac{l!}{N!} f^{(N-l)}(z) = z^l + \binom{l}{1} a_1 z^{l-1} + \binom{l}{2} a_2 z^{l-2} + \cdots + \binom{l}{k} a_k z^{l-k} + \cdots + \binom{l}{1} a_{l-1} z + a_l.$

Observe that $v_p(a_1) \geq 0$ because $-a_1$ (the center of mass of f) is one of the roots of f. Once again following the proof of [4, Proposition 9] and using equality (5) with $l = 2, \cdots, N - 2$ and z the common root of $f^{(N-l)}$ and f, we prove by induction on l that

(6) $$v_p(a_l) \geq 0 \quad \text{for all } l = 2, \cdots, N - 2.$$

Let z_j be such that $v_p(z_j) = 0$. The equality

$$-N a_1 z_j^{N-1} = z_j^N + \binom{N}{2} a_2 z_j^{N-2} + \cdots + \binom{N}{k} a_k z_j^{N-k} + \cdots + \binom{N}{2} a_{N-2} z_j^2$$

shows that $v_p(a_1) = 0$. Therefore, we may assume without loss of generality that $a_1 = -1$. Then we can write $f(z) = (z - 1)g(z)$ where

$$g(z) = \left(z^{N-1} - (N-1)z^{N-2} + (\binom{N}{2} a_2 - (N-1))z^{N-3} + \right.$$

$$\left. (\binom{N}{3} a_3 + \binom{N}{2} a_2 - (N-1))z^{N-4} + \cdots + (\binom{N}{3} a_{N-3} + \cdots + \binom{N}{2} a_2 - (N-1))z^2 \right).$$

In view of (6) and Lemma 5, all roots of g have strictly positive valuations (actually greater than $1/(N-3)$). As a consequence, we see that 1 is a simple root of of f and that $v_p(z_j) > 0$ for $j = 1, \cdots, N - 3$.

Whenever $f^{(N-l)}(1) \neq 0$, the Casas-Alvero property implies that $f^{(N-l)}(z_j) = 0$ with $v_p(z_j) > 0$ and from equality (5) we get $v_p(a_l) > 0$.

But as

$$f(1) = 1 - N + \binom{N}{2} a_2 + \cdots + \binom{N}{k} a_k + \cdots + \binom{N}{2} a_{N-2} = 0,$$

there is at least one index $2 \leq l \leq N - 2$ such that $v_p(a_l) = 0$. In other words, at least one of the derivatives $f^{(N-l)}(1) = 0$. If we put this result together with Proposition 1, we get :

Lemma 6. *Let f be a non-trivial CA-polynomial of degree $N = p + 1$, p prime. Let c be the center of mass of f. Then the following conditions are satisfied :*
- $f^{(N-1)}(c) = 0$,
- $f^{(l)}(c) \neq 0$ *for at least one $l \in \{2, \cdots, N - 2\}$,*
- $f^{(k)}(c) = 0$ *for at least one $k \in \{2, \cdots, N - 2\}$.*

Let us now go further into the investigation of the orders of the derivatives having the center of mass as a root.

We may again assume that f is of the form (4) and that $a_1 = -1$.

For the sake of clarity, we will use the notation $x \equiv y$ if $v_p(x - y) > 0$.

In view of Lemma 6, let $l_1 < l_2 < \cdots < l_m$ be the indices between 2 and $N - 2$ such that $f^{(N-l_j)}(1) = 0$, $j = 1, \cdots, m$.

As observed previously, for all $k \in \{2, \cdots, N-2\}$, we have $v_p(a_k) \geq 0$. Moreover, if $k \notin \{l_1, \cdots, l_m\}$, $a_k \equiv 0$.

From equality (5) with $z = 1$ and $l = l_1, l_2 \cdots, l_m$, we get

$$(7) \quad \begin{cases} 1 - l_1 + a_{l_1} & \equiv 0 \\ 1 - l_2 + \binom{l_2}{l_1}a_{l_1} + a_{l_2} & \equiv 0 \\ \quad \vdots & \\ 1 - l_m + \binom{l_m}{l_1}a_{l_1} + \binom{l_m}{l_2}a_{l_2} + \cdots + a_{l_m} & \equiv 0 \end{cases}$$

Now, using that $\frac{f(1)}{p} = 0$ and that $v_p(\binom{k}{N}) \geq 1$ for $k = 2, \cdots, N-2$, we obtain

$$(8) \quad -1 + \frac{\binom{N}{l_1}}{p}a_{l_1} + \cdots + \frac{\binom{N}{l_m}}{p}a_{l_m} \equiv 0.$$

Now observe that for all $2 \leq l \leq N - 2$, we have :

$$\begin{aligned} \frac{\binom{N}{l}}{p} &= \frac{N(N-2)(N-3)\cdots(N-(l-1))}{l!} \\ &= \frac{(p+1)(p-1)(p-2)\cdots(p-(l-2))}{l!} \\ &= \frac{1}{l!}(p^{l-1} + \alpha_{l-2}p^{l-2} + \cdots + \alpha_1 p) + \frac{(-1)^{l-2}(l-2)!}{l!} \end{aligned}$$

where $\alpha_1, \cdots, \alpha_{l-2}$ are integers.

Therefore:

$$\frac{\binom{N}{l}}{p} \equiv \frac{(-1)^l}{l(l-1)}.$$

Putting equations (7) and (8) together and putting $\tilde{a}_{l_j} = \frac{a_{l_j}}{l_j(l_j-1)}$, we obtain:

$$(9) \quad \begin{cases} -1 + l_1\tilde{a}_{l_1} & \equiv 0 \\ -1 + \binom{l_2-2}{l_1-2}l_2\tilde{a}_{l_1} + l_2\tilde{a}_{l_2} & \equiv 0 \\ \quad \vdots & \\ -1 + \binom{l_m-2}{l_1-2}l_m\tilde{a}_{l_1} + \binom{l_m-2}{l_2-2}l_m\tilde{a}_{l_2} + \cdots + l_m\tilde{a}_{l_m} & \equiv 0 \\ -1 + (-1)^{l_1}a_{l_1} + (-1)^{l_2}\tilde{a}_{l_2} + \cdots + (-1)^{l_m}\tilde{a}_{l_m} & \equiv 0. \end{cases}$$

Let us define the determinant

$$(10) \quad \Delta = \begin{bmatrix} -1 & l_1 & 0 & 0 & \cdots & 0 \\ -1 & \binom{l_2-2}{l_1-2}l_2 & l_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ -1 & \binom{l_m-2}{l_1-2}l_m & \binom{l_m-2}{l_2-2}l_m & & \cdots & l_m \\ -1 & (-1)^{l_1} & (-1)^{l_2} & & \cdots & (-1)^{l_m} \end{bmatrix}.$$

We see that necessarily $\Delta = 0$. Otherwise, inverting (9), we would get in particular that $1 \equiv 0$. Let us summarize this result by:

Lemma 7. *Let f be a Casas-Alvero polynomial of the form (4) with $a_1 = -1$. Let $l_1 < l_2 < \cdots < l_m$ be the indices between 2 and $N-2$ such that $f^{(N-l_j)}(1) = 0$, $j = 1, \cdots, m$ and let Δ the determinant defined by (10). Then p divides Δ.*

Proposition 7. *Let f be a non-trivial CA-polynomial of degree $N = p + 1$, p prime. Then there are at least two indices $2 \leq l_1 < l_2 \leq N - 2$ such that $f^{(l_1)}(c) = f^{(l_2)}(c) = 0$.*

Proof. If not, in virtue of Lemma 6, there exists a unique index $2 \leq l \leq N - 2$ such that $f^{(N-l)}(c) = 0$.

We can assume without loss of generality that f is of the form (4) with $a_1 = -1$ and apply Lemma 7. Then $m = 1$ and

$$(11) \qquad \Delta = \begin{bmatrix} -1 & l \\ -1 & (-1)^l \end{bmatrix} = l - (-1)^l.$$

Observe that $1 \leq l - (-1)^l \leq l + 1 \leq N - 2$ for $l \in 2, \cdots, N - 3$.
Besides, $N - 2 - (-1)^{N-2} = N - 3$ because N is even.
Finally, there is no way for p to divide Δ and this contradicts Lemma 7. $\qquad \square$

Remark 7. *We can actually go a bit further, but the results are not as conclusive. For instance, let f be a CA-polynomial of degree $N = 12$, and suppose there are exactly two indices $2 \leq l_1 < l_2 < N - 1$ such that $f^{(l_1)}$, $f^{(l_2)}$ and $f^{(N-1)}$ have a common root. Then applying Lemma 7, we can check that there are only 4 possibilities for (l_1, l_2): (l_1, l_2) must be $(3, 8)$, $(5, 6)$, $(6, 8)$ or $(6, 9)$.*

Remark 8. *In [2], Castryck defines the* type *of a CA-polynomial f of degree N as follows: Let $\{\alpha_1, \ldots, \alpha_k\}$ denote the roots of f. A subset $S \subset \{\alpha_1, \ldots, \alpha_k\}$ is called* covering *if for each $i = 1, \ldots, N - 1$, there exists $\alpha \in S$ such that $f^{(i)}(\alpha) = 0$. The type of f is defined as*

$$type(f) = \min\{Card\ S - 1,\ S\ covering\}.$$

Castryck establishes that

$$2 \leq type(f) \leq N - 3$$

for any non-trivial CA-polynomial f ([2]; the lower bound follows from Proposition 1). Our result Proposition 7 gives something more: any CA-polynomial f of degree $N = p + 1$ satisfies

$$type(f) \leq N - 4.$$

In particular, for $N = 12$, this bound combined with the results of Castryck (loc. cit.) implies that in order to prove the Casas-Alvero conjecture in degree 12, the only cases remaining to be checked are polynomials of type 6, 7 and 8.

Our final result proves the Casas-Alvero conjecture for degree $p + 1$ polynomials whose roots are rational numbers:

Proposition 8. *There is no non-trivial CA-polynomial of degree $N = p + 1$, $p \geq 3$ prime, with rational roots.*

Proof. Using the same notations as in the proof of Lemma 4, we may assume that f is of the form

$$
f(z) = z^N - N z^{N-1} + \binom{N}{2} z^{N-2}
$$

$$
+ \cdots + (-1)^{k-1} \binom{N}{k-1} z^{N-k+1} + \binom{N}{k} a_k z^{N-k} + \cdots + \binom{N}{2} a_{N-2} z^2,
$$

with $v_p(z_j) \geq 1$ for $j = 1, \cdots, N-3$. Here, we have denoted by k the smallest index between 2 and $N-2$ such that $f^{(N-k)}(1) \neq 0$ (we know from Lemma 4 such a k exists).

We introduce the notation

$$
S_m = \sum_{j=1}^{N-3} z_j^m.
$$

Then we have: $v_p(S_1) = v_p(N-1) = 1$, and $v_p(S_j) \geq 2$ for $j = 2, \cdots, N-2$. Using Newton formulas (see Lemma 2, $l = 0$), we obtain

$$
-k \binom{N}{k} a_k = \sum_{j=0}^{k-1} (-1)^j (1 + S_{k-j}) \binom{N}{j}
$$

$$
= \sum_{j=0}^{k-1} (-1)^j \binom{N}{j} + \sum_{j=0}^{k-1} (-1)^j S_{k-j} \binom{N}{j}
$$

$$
= (-1)^{k-1} \binom{N-1}{k-1} + \sum_{j=0}^{k-1} (-1)^j S_{k-j} \binom{N}{j}.
$$

Note that $v_p(\binom{N}{k} a_k) > 1$ which will lead to a contradiction:

Case 1: $k = 2$. The last equality becomes :

$$
-2 \binom{N}{2} a_2 = -(N-1) + S_2 - N S_1 = -(N-1) + S_2 - N(N-1) = -(N+1)(N-1) + S_2.
$$

The valuation of the right-hand term is 1.

Case 2: $3 \leq k \leq N-2$: The right-hand term is

$$
(-1)^{k-1} \binom{N-1}{k-1} + \sum_{j=0}^{k-2} (-1)^j S_{k-j} \binom{N}{j} + (-1)^{k-1} S_1 \binom{N}{k-1}.
$$

But $v_p(S_{k-j}) \geq 2$ for $j = 0, \cdots, k-2$, and $v_p(S_1 \binom{N}{k-1}) = 2$, so the valuation of the right-hand term is $v_p(\binom{N-1}{k-1}) = 1$.

$\square$

3. A FINAL REMARK ABOUT A POSSIBLE COUNTEREXAMPLE IN DEGREE 12

Proposition 9. *Let f be a non-trivial CA-polynomial of degree $N \geq 1$.*

  1) *Assume that some prime $q \geq 2$ divides all binomial coefficients $\binom{N}{k}$, $k = 1, \cdots, N-1$ except for $k = q^s$ and $k = N - q^s = q^t$, $s, t \in \mathbb{N}$. Then the derivatives $f^{(q^s)}$ and $f^{(N-q^s)}$ don't have any common root.*

  2) *Assume that some prime $q \geq 2$ divides all binomial coefficients $\binom{N}{k}$, $k = 1, \cdots, N-1$ except for $k = l_1, \cdots, l_m$. Then there is no $a \in \mathbb{C}$ such that*

$$f(a) = f^{l_1}(a) = \cdots = f^{l_m}(0).$$

Remark 9. *1) This implies in particular that $s \neq t$. This means that there doesn't exist a nontrivial CA-polynomial with degree $N = 2q^r$, q prime. But this result is already proved in [5].*

Proof.   1) We may assume that $s \leq t$ and that f and its derivatives are of the form :

$$(12) \qquad \frac{l!}{N!} f^{(N-l)}(z) = z^l + \binom{l}{1} a_1 z^{l-1} + \cdots + \binom{l}{1} a_{l-1} z + a_l,$$

with $a_N = a_{q^s} = 0$ and $\min\{v_q(z_j),\ j = 1, \cdots, N\} = 0$ where we have denoted by $z_1, \cdots, z_N$ the roots of f.

As in [4, Proposition 9], using equality (12) with $l = 1, \cdots, N-1$ and z the common root of $f^{(N-l)}$ and f, we prove by induction on l that

$$(13) \qquad v_q(a_l) \geq 0 \quad \text{for all } l = 1, \cdots, N.$$

Using $f(z_j) = 0$ with $v_q(z_j) = 0$, we deduce that $v_q(a_{q^t}) = 0$.

Now we apply formula (12) with $l = q^s$ then $l = N - q^s$. We find, with the help of Lemma 4, that all roots of $f^{(N-q^s)}$ have q-valuation > 0 while all roots of $f^{(q^s)}$ have q-valuation $= 0$.

  2) We proceed by contradiction. Let us repeat the beginning of the proof in 1) but this time assuming that $a_N = a_{l_1} = \cdots = a_{l_m} = 0$. We still get

$$(14) \qquad v_q(a_l) \geq 0 \quad \text{for all } l = 1, \cdots, N.$$

Using $f(z_j) = 0$ with $v_q(z_j) = 0$ we have

$$-z_j^N = \binom{N}{1} a_1 z_j^{N-1} + \cdots + \binom{N}{N-1} a_{N-1} z_j.$$

But by assumption, the q-valuation of the right-hand term is ≥ 1 and we reach a contradiction.

$\square$

Remark 10 (Case N=12). *Observe that 2 (respectively 3) divides $\binom{12}{k}$, $k = 1, \cdots, 11$, except for $k = 4, 8$ (resp. k=3,9). Thus, a possible counterexample in degree 12 should satisfy : $f^{(4)}$ and $f^{(8)}$ (respectively $f^{(3)}$ and $f^{(9)}$) don't share any root.*

References

[1] E. Casas-Alvero, *Higher order polar germs*, Journal of Algebra 240(1) (2001), 326–337,

[2] W. Castryck, *Revisiting the computational approach to the Casas-Alvero conjecture*, preprint 27-02-2012,

[3] G. Diaz-Toca and L. Gonzalez-Vega, *On a conjecture about univariate polynomials and their roots*. In Algorithmic Algebra and Logic 2005 (A. Dolzmann, A. Seidl and T. Sturm, eds.), Norderstedt 2005,

[4] J. Draisma and J. P. de Jong, *On the Casas-Alvero conjecture*, EMS Newsletter June 2011, 29–33,

[5] H.-C. Graf von Bothmer, O. Labs, J. Schicho and C. van de Woestijne, *The Casas-Alvero conjecture for infinitely many degrees*, Journal of Algebra 316(1) (2007), 224–230,

[6] J. P. de Jong, *Het Casas-Alvero vermoeden*, 19-04-2010,

[7] V. V. Prasolov, *Polynomials*, Algorithms and Computation in Mathematics **Volume 11** Springer,

[8] A. Sudbury, *The number of distinct roots of a polynomial and its derivatives*, Bull. London Math. Soc., 5 (1973), 13–17,

[9] V. P. Kostov and B.Z. Shapiro, *On arrangements of roots for a real hyperbolic polynomial and its derivatives* Bull. Sci. math. **Volume 126** (2002), 45–60,

[10] P. Ribenboim, *The theory of classical valuations*, Springer Monographs in Mathematics, Springer–Verlag New York Berlin Heidelberg 1999,

[11] H. Verhoek, *Some remarks about a polynomial conjecture of Casas-Alvero*, Séminaire Bourbakettes, Paris 2009,

INSTITUT DE RECHERCHE MATHÉMATIQUE AVANCÉE, UNIVERSITÉ LOUIS PASTEUR 7 RUE RENÉ DESCARTES, 67084 STRASBOURG CEDEX, FRANCE.
E-mail address: robert.laterveer@math.unistra.fr

INSTITUT DE RECHERCHE MATHÉMATIQUE AVANCÉE, UNIVERSITÉ DE STRASBOURG 7 RUE RENÉ DESCARTES, 67084 STRASBOURG CEDEX, FRANCE.
E-mail address: myriam.ounaies@math.unistra.fr